



(19)

Europäisches Patentamt  
European Patent Office  
Office européen des brevets



(11)

EP 0 866 615 A2

(12)

## EUROPEAN PATENT APPLICATION

(43) Date of publication:  
23.09.1998 Bulletin 1998/39

(51) Int Cl. 6: H04N 7/167

(21) Application number: 98301685.8

(22) Date of filing: 06.03.1998

(84) Designated Contracting States:  
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC  
NL PT SE  
Designated Extension States:  
AL LT LV MK RO SI

(30) Priority: 19.03.1997 JP 66538/97

(71) Applicant: SONY CORPORATION  
Tokyo 141 (JP)

(72) Inventor: Sato, Masahiko  
Shinagawa-ku, Tokyo 141 (JP)

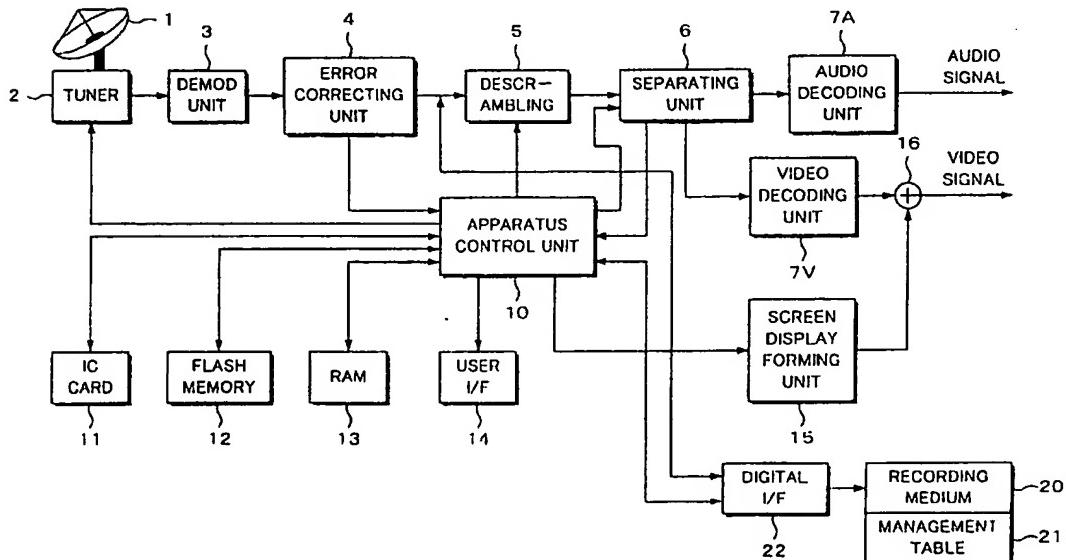
(74) Representative: Turner, James Arthur et al  
D. Young & Co.,  
21 New Fetter Lane  
London EC4A 1DA (GB)

## (54) Data transmission and reception

(57) Video and audio data of a plurality of received programs and a common information ECM are recorded to a recording medium. A recording position of the program is written on a management table. When reproducing a desired one of the recorded programs, the ECM is also reproduced together with the video and audio data. The data to retrieve the desired program and

an individual information EMM are transmitted through a broadcasting wave. To descramble the reproduced video and audio data, the reproduced ECM and the received EMM are used. Since the individual information EMM is the latest information, even if there is a time lag between the recording time point and the reproducing time point, the reliability of the conditional access is not deteriorated.

Fig. 1



EP 0 866 615 A2

## Description

This invention relates to data transmission and reception.

Recently, a digital broadcasting system for transmitting multimedia data such as image signals, audio signals, and the like by using a communication satellite has been being put into practical use. Fig. 4 shows an outline of a typical digital broadcasting system. The transmission side of a program is made up of an up-link station, a program provider, and a management system.

Video and audio data from a program provider 101 is supplied to an encoder and multiplexer 103 of the MPEG (Moving Pictures Expert Group) 2 of an up-link station 102. In the MPEG 2 encoder and multiplexer 103, the video and audio data is compressed and the compressed video and audio data is stored in a packet of a length of 188 bytes. A plurality of programs and the packets of the respective corresponding video and audio data are multiplexed, so that a transport packet of the MPEG2 is formed. A transport stream is formed by a series of transport packets. The number of transport streams corresponds to the number of transponders installed in the communication satellite.

The MPEG2 transport stream is supplied to a transmission system 104. In the transmission system 104, processes such as scrambling process of every packet, error correction encoding of every packet, modulation, and the like are executed and a modulation output is supplied to a transmitting antenna 105. The scrambling process is necessary to realize a conditional access which is used to control about the permission or inhibition of the monitoring every viewer. In the scrambling process, for example, a contract of a pay-per-view in which only a certain program is monitored with a toll every time can be made. A key to descramble is supplied from a key management system 106 to the MPEG2 encoder and multiplexer 103 and has been inserted as one of the packets into the transport stream in a manner similar to the video and audio information.

An integrated management of the MPEG2 packets is performed by a program management system 107. The program management system 107 and key management system 106 are unified, thereby encrypting the key to descramble. Further, in a customer management system 108, items regarding a monitor contract or the like are managed. Viewer information is transmitted and received between the customer management system and the home of the viewer via a telephone line 109.

A broadcasting radio wave transmitted from the transmitting antenna 105 through a communication satellite 110 is received by a receiving antenna 111 at each home. A receiver 112 is connected to the receiving antenna 111. The receiver 112 is constructed by a tuner for designating a receiving transponder, a demodulating unit, a descrambling unit for descrambling, a demultiplexer for designating a packet to be separated, a video decoding unit, an audio decoding unit, and the like. The

decoded video and audio signals are supplied to a television receiver 113.

A key for descrambling is encrypted and transmitted as concerned information together with video and audio signals. The key to decrypt the encryption has been stored in an IC card 114 inserted in the receiver 112. Which program can be descrambled can be controlled from the transmission side on the basis of contract information of each reception system. The receiver having a conditional accessing function is usually called an IRD (Integrated Receiver/Decoder).

The above digital satellite broadcasting system is not limited to an application field such that a television broadcasting is merely monitored but can be also used as a transmission system of digital data of a large capacity by many channels. That is, the receiver of the digital satellite broadcasting can have a function as a receiving apparatus of digital data such as video and audio data, data for a computer, or the like.

As one of using methods of the digital satellite broadcasting, there is considered a method whereby by combining a receiver and a recording medium of a large capacity, a large quantity of reception data can be accumulated. For example, the reception data is recorded at night when a transmitting line is relatively free, and a desired portion is reproduced from the recorded data later. As a recording medium of a large capacity, a digital VCR, a hard disk, an optical disk, a semiconductor memory, or the like can be used.

In the digital satellite broadcasting, although a form in which a monitor contract is made on a channel unit basis, a form (pay-per-view) in which a fee of only the monitored programs is paid, and the like exist, it is generally a toll broadcasting and the conditional access is used. Therefore, according to the method whereby reception data has previously been stored in the memory of the large capacity and the desired program is reproduced later, it is irrational that all of the programs which are stored are charged. The programs which were selectively read out from the memory and were reproduced are charged.

The monitor control in the toll broadcasting system is performed by a scramble authorization system. In this system, individual information (EMM: Entitlement Management Message) that was formed on the transmission side and is peculiar to the receiving terminal is sent to the viewer. On the receiving terminal, the EMM of the same ID as the own ID is decrypted, and a work key is fetched into the IC card. The key to decode the EMM is a key which is individual for each receiving terminal and has previously been stored in the IC card. Further, a contracted channel ID and a contract type (temporary contract, pay-per-view, or the like) in addition to the work key are included in the EMM.

When a program is monitored, common information (ECM: Entitlement Control Message) which is accompanied with the program and is common for the receiving terminals is fetched into the IC card. If the work key

corresponding to this channel has previously been stored, a descrambling is performed and can be monitored. The EMM and the common information (hereinafter, referred to as an ECM) are transmitted in a form of the packet of the transport stream of the MPEG2 in a manner similar to the video and audio data. In case of the pay-per-view, the monitor information is periodically up-loaded through the telephone line.

In the foregoing toll broadcasting system, as one of methods of realizing a method whereby the recording medium (large capacity memory) is combined to the receiver and a desired one of the programs stored in the recording medium is selectively reproduced and only the reproduced program is charged, a method of recording the EMM and ECM as well to the recording medium is also considered. The video and audio data of a plurality of programs are recorded in a scrambled state (form of the packet) on the recording medium, the video and audio data which was selectively reproduced is descrambled by the system of the receiver, and is further decoded. In order to enable the descrambling, the EMM and ECM are recorded to the recording medium.

However, a time lag exists between the timing when recording the reception data to the recording medium and the timing when reproducing it later. There is a possibility such that the EMM which is individual for each receiving terminal is changed due to a change or the like in contract. Thus, according to the system for recording the EMM at that time point together with the data of the program, there occurs a fear such that the reliability of the conditional access is deteriorated. For example, upon recording, although the customer which is instructed in the EMM has a right corresponding to the rank of the recorded program, at the time of point of reproduction, even if the right has already been terminated due to the elapse of the validity term, the right is authorized on the EMM which has already been recorded. In an extreme case, a situation such that the right which was validated by the latest EMM is invalidated by the reproduced old EMM also occurs.

Various respective aspects and features of the invention are defined in the appended claims.

Embodiments of the invention can provide a data transmitting apparatus, a receiving apparatus, and a data transmission and reception system which can prevent a situation such that the reliability of a conditional access is deteriorated by controlling the reproduction of recorded data by latest individual information.

According to a preferred embodiment of the invention, to address the foregoing problems, there is provided a data transmitting apparatus for transmitting multiplexed digital data, characterized by comprising:

means for encrypting a plurality of information data;  
means for transmitting first control data which is used to decrypt the encryption and is common to receiving terminals and second control data which is used to decrypt the encryption and is individual

5 for the receiving terminals together with the plurality of encrypted information data; and  
means for transmitting data necessary to retrieve the plurality of information data and the present second control data after the plurality of encrypted information data was transmitted.

10 According to another preferred embodiment of the invention, there is also provided a data receiving apparatus for receiving multiplexed digital data, characterized in that

15 a plurality of encrypted information data, first control data which is used to decrypt the encryption and is common to receiving terminals, and second control data which is used to decrypt the encryption and is individual for the receiving terminals are included in a reception signal,  
20 and the apparatus comprises:

25 a recording medium for recording the plurality of encrypted information data and the first control data;  
managing means for instructing a recording position of each of the plurality of information data on the recording medium;  
means for reproducing desired information data and the first control data from the recording medium with reference to the managing means; and  
30 means for decrypting the reproduced information data by using the reproduced first control data and the present second control data received.

35 According to another preferred embodiment of the invention, there is further provided a data transmission and reception system for transmitting multiplexed digital data and receiving the multiplexed digital data, characterized in that

40 an apparatus on the transmission side comprises:

45 means for encrypting a plurality of information data; and  
means for transmitting first control data which is used to decrypt and is common to receiving terminals and second control data which is used to decrypt and is individual for the receiving terminals together with the plurality of encrypted information data,  
50 and an apparatus on the reception side comprises:

55 a recording medium for recording the plurality of encrypted information data and the first control data,  
managing means for instructing a record-

ing position of each of the plurality of information data on the recording medium; means for reproducing desired information data and the first control data from the recording medium with reference to the managing means; and means for decrypting the reproduced information data by using the reproduced first control data and the present second control data received.

According to the transmitting apparatus of embodiments of the invention, since the date for retrieving a plurality of information data and the second control data EMM are transmitted, the plurality of information data can be easily retrieved on the reception side. Since the encryption is decrypted by the latest EMM on the reception side, the reliability of the conditional access is not deteriorated. In embodiments of the receiving apparatus, the plurality of information data received and the first control data ECM are recorded to the recording medium and the reproduced first control data ECM and the received second control data EMM are used to decrypt the information data which was selectively reproduced, so that the deterioration of the reliability of the conditional access can be prevented.

The invention will now be described by way of example with reference to the accompanying drawings, throughout which like parts are referred to by like references, and in which:

- Fig. 1 is a block diagram showing a construction of an embodiment of the invention;
- Fig. 2 is a block diagram showing a construction mainly about the monitor control in the embodiment of the invention;
- Fig. 3 is a schematic diagram for explaining the retrieving operation in the embodiment of the invention; and
- Fig. 4 is a schematic diagram showing an outline of a typical digital broadcasting system.

An embodiment of the invention will now be described hereinbelow with reference to the drawings. Fig. 1 is a block diagram showing the embodiment. A receiving antenna shown at 1 receives a radio wave from a communication satellite (or broadcasting satellite). A converter associated with the antenna 1 down-converts the reception signal into a first IF (intermediate frequency) signal of a predetermined frequency and generates to a tuner 2.

In the tuner 2, a receiving channel (namely, receiving transponder) set by the user is selected and a second IF signal is formed. The second IF signal is supplied to a demodulating unit 3 and, for example, a QPSK is demodulated. A demodulation output from the demodulating unit 3 is supplied to an error correcting unit 4. The error correcting unit 4 corrects errors occurring dur-

ing the transmission by an error correction code such as a Reed Solomon code. An output (transport stream) of the error correcting unit 4 is supplied to a descrambling unit 5. In the descrambling unit 5, a descramble to cancel the scramble is performed.

The transport stream of the MPEG2 which is an output of the descrambling unit 5 is supplied to a separating unit 6. In the separating unit 6, the packet of a desired channel is separated from the transport stream. It is also separated into video data, audio data, and control data (the ECM and EMM and the like are included) on the basis of information of a header portion. Further, a switching between the data of the received program and the data of the program which was selectively reproduced from the recording medium is also performed.

The video data from the separating unit 6 is decoded by a video decoding unit 7V and a reception video signal is generated. The audio data is decoded by an audio decoding unit 7A and a reception audio signal is generated. The control data (including the EMM and ECM) is supplied to an apparatus control unit 10. The decoded video signal is added with a signal for display by an adder 16. An output video signal of the adder 16 is displayed on a display (not shown). Similarly, the decoded audio signal is, for instance, amplified by an amplifier and outputted from a speaker (not shown). A PID is added to the transport packet and a transmission destination (video decoding unit 7V, audio decoding unit 7A, or apparatus control unit 10) of the packet is instructed by the PID.

The apparatus control unit 10 controls the operation of the whole receiver and is constructed by a microcomputer. The tuner 2, an IC card 11, a flash memory 12, a RAM 13, a user interface 14, and a screen display forming unit 15 are connected to the apparatus control unit 10. Further, bit error rate information is supplied from the error correcting unit 4 to the apparatus control unit 10. Since a bit error rate has a correlation with a C/N ratio, the apparatus control unit 10 can know a radio wave situation (C/N ratio) from the bit error rate information. A degree of C/N ratio can be displayed on the screen of the display. Thus, the adjustment of the direction of the antenna, permission or inhibition of the downloading of the program, and the like can be controlled.

The user interface 14 is keys on a front panel, a pointing device such as screen display, mouse, or the like, a remote control system, or the like. Although not shown, a modem is connected to the apparatus control unit 10 and viewer information is transmitted via the telephone line.

A program for controlling the ordinary operation is stored in the flash memory 12. The control of the ordinary operation which is executed by the apparatus control unit 10 is executed on the basis of the program stored in the flash memory 12. The RAM 13 is used as a temporary storing unit when rewriting the flash memory 12. The screen display forming unit 15 forms various display signals under the control of the apparatus con-

trol unit 10. The display signals are supplied to the adder 16 and multiplexed to the decoded video signal.

A recording medium 20 is connected to the receiver through a digital interface 22 in order to record the data of a plurality of programs received by the receiver by using free time such as at night or the like as mentioned above and to selectively reproduce a desired program among them after that. As a recording medium 20, a medium of a large capacity is preferable and a digital VCR (video cassette tape recorder), a hard disk, an optical disk, or the like can be used. A management table 21 is used in association with the recording medium 20. The management table 21 shows a corresponding relation between the recorded data, for example, an ID (program number) of the program and information of its recording position. Although a control unit, a mechanism unit, and the like are provided in association with the recording medium 20, they are not shown for simplicity of explanation.

As a management table 21, an area on the same medium as that of the recording medium 20 can be used or an area on another medium can be also used. For example, in case of the digital VCR, the management table can be constructed in a semiconductor memory built in a cassette or a surface of the cassette. In case of the semiconductor memory, a directory area on the memory can be used.

The previous data of the descrambling unit 5, namely, the video and audio data in the scrambled state is recorded on the recording medium 20 through the digital interface 22. The apparatus control unit 10 and digital interface 22 are connected and the ECM associated with the video and audio data of the program to be recorded is also recorded. Since the ECM and EMM are information for control, they are not scrambled. However, the EMM as individual control data is not recorded in the receiver. This is because the EMM received at the newest real time is to be used as the EMM.

Further, control information necessary to record and reproduce the data to/from the recording medium 20 is also transmitted from the apparatus control unit 10 through the digital interface 22. The reproduced data, namely, the video data and audio data of the selected program are supplied to the descrambling unit 5 through the digital interface 22. The reproduced ECM associated with the selected program is supplied to the apparatus control unit 10 through the digital interface 22. By using the reproduced ECM and the received present (namely, latest) EMM, the apparatus control unit 10 generates a scramble key that is necessary for descrambling the reproduced video and audio data. Thus, the descrambled video and audio data is obtained.

Although the digital satellite broadcasting system is constructed in a manner similar to that shown in Fig. 4, a more detailed construction mainly about the monitor control in the toll broadcasting is shown in Fig. 2. Fig. 2 shows a transmission side system and a reception side system. Both systems are connected by a transmission

path 31 including a communication satellite, a broadcasting satellite, and the like and a telephone line 32 to up-load the monitor information.

The transmission side system will now be described. An encoder 33 converts the video signal and audio signal into digital signals and compresses the digital signals. Specifically speaking, for example, an MPEG2 encoder is used. An output of the encoder 33 is supplied to a multiplexing unit 34. In the multiplexing unit 34, the output of the encoder 33 and the control information are time-division multiplexed. A scrambling unit 35 scrambles the digital information by the scramble key. The EMM and ECM serving as control information are not scrambled.

The EMM is transmitted to the individual receiver and the ECM is the information associated with the program and they are the signals which are commonly transmitted to the program receiver. In a concerned information transmitting unit 36, the scramble key is encrypted by the work key and is transmitted as a part of the ECM. The work key is encrypted in a scramble management system 37 by an individual key peculiar to the receiver and is transmitted as a part of the EMM. In the scramble management system 37, the individual key is stored in correspondence to all of the receivers. That is, the scramble management system 37 receives the data of the EMM from a customer management system 38 and encrypts the data. In the scramble management system 37, a card ID, the individual key, and all of the circulated work keys are stored. A card ID and an individual key are newly generated and transferred to an IC card issuer, thereby allowing an IC card to be formed.

A customer management system 38 processes the monitor information which is up-linked from a number of receivers and contract requests from the viewers and transfers the contract information to the scramble management system 37. A program management system 39 controls the encoder 33 by the control signal in accordance with the program. And the program management system 39 generates a program number or one like, and supplies to the concerned information transmitting unit 36. The concerned information transmitting unit 36 mainly receives the ECM and encrypts.

On the receiver side, the EMM is previously fetched to an IC card 41 (shown at reference numeral 11 in Fig. 1) as one of security modules and is decoded by the EMM recorded in the IC card 41. The work key is taken out and stored in the IC card 41. The contract information in the EMM is stored.

In case of receiving a certain program, the receiver reads the ECM associated with the program into the IC card 41 and is collated with the contract information which has previously been fetched. If the received program is the contracted program, the scramble key in the ECM is decoded by using the work key and sent to a decoder 42. In the decoder 42, a descrambling is performed by an internal descrambling unit.

In case of the pay-per-view contract, a monitor ca-

reer is stored in the IC card 41. After the elapse of a predetermined period, the monitor career is up-linked as monitor information to the customer management system 38 of the transmission side system through a telephone modem in the decoder 42. The IC card uses, for example, an 8-bit CPU of one chip. The individual key and the ID have been written in an EEPROM in the chip and cannot be rewritten by the user. The monitor information is also written in the EEPROM.

The control of the monitor control system in he toll broadcasting mentioned above will now be described. The descrambling is constructed by processes of three stages. First, the work key is decoded from the EMM by using the individual key of the receiver. Subsequently, the scramble key is decoded from the ECM by using the work key. The video data and audio data are descrambled by using the decoded scramble key.

When explaining in more detail, the EMM is transmitted to the viewer who normally made a contract, the encryption is decrypted by the first decoder, and the work key is stored into the IC card 41. The key which is used in the decoding is the key that is individual for each receiver. The individual key has previously been stored in the IC card 41. In the transmission side system, as mentioned above, the individual keys of the receivers and all of the ID numbers have been stored and the encrypted EMM is transmitted by using the individual key corresponding to the ID number of the receiver to be transmitted. The ID number has been added to the non-encrypting portion of the EMM. In the receiver, the ID number is compared with the ID in the IC card 41. Only the EMM in which those IDs coincide is fetched into the IC card 41 and used.

When the program is monitored, the ECM associated with the program is fetched to the IC card 41. If the work key corresponding to the channel has previously been stored, the second decoder operates and the scramble key is obtained. The scrambled program signal is descrambled in the descrambling unit and is outputted as a signal which can be normally monitored.

Information of the work key, contracted channel ID, and contract type (temporary contract, paper-view, or the like) is included in the EMM. The work key is sent together with the key number and a plurality of work keys can be selectively used.

According to the embodiment of the invention, in a plurality of received program data, the packet of the video data and the packet of the audio data of the scrambled information and the ECM associated with the program are stored into the recording medium 20 through the digital interface 22. In this case, a corresponding relation between the program number as an ID of the program and the recording position of the program on the recording medium 20 is also recorded in the management table 21 concerned with the recording medium 20. The EMM having a possibility such that it will be changed in future by a change in contracted contents or the like is not recorded onto the recording medium 20.

After the recording to the recording medium 20, data for retrieving (browsing) the recorded information data is transmitted from an up-link station to the receiver. At the same time, the EMM as an individual information 5 is also annexed and transmitted to the viewer who recorded the program. Processes in case of selectively reproducing the desired program from the recording medium 20 will now be described with reference to Fig. 3.

By the data for browsing sent from the up-link station to the viewer, contents as shown at 51 in Fig. 3 are displayed on the display of the viewer. That is, characters showing the contents 52 of the plurality of recorded programs and the buttons 53 for selection are included. The display 51 shown in Fig. 3 is one example. As another example, so long as a display such that the contents of the recorded programs are displayed and a desired one of the recorded programs can be selected, various displays can be used. The browser (software) has previously been stored as a program in the ROM of the receiver or is transmitted through the broadcasting wave and is down-loaded into the memory which is connected to the apparatus control unit 10.

The viewer designates a desired program to be reproduced by using a mouse or the like in the display 51 for browsing. When a certain program is designated, the program number corresponding to the program is supplied from the apparatus control unit 10 to the management table 21 through the digital interface 22, for example. As shown in Fig. 3, recording positions (start addresses ST1, ST2, ..., and end addresses EN1, EN2, ...) 25 on the recording medium 20 of program numbers X1, X2, ... of the programs recorded on the recording medium 20 have been written in the management table 21. Therefore, by referring to the management table 21, the recording position of the program number designated in the display 51 of the browsing can be known.

The information of the desired program number and the corresponding recording position is sent to the recording medium 20 (more specifically speaking, reading 40 or reproduction control unit). Thus, the video packet, audio packet, and ECM of the program of the desired program number are reproduced. The reproduced information is transmitted to the apparatus control unit 10 through the digital interface 22. In the apparatus control unit 10, the scramble key is generated as mentioned above by using the received latest EMM and the reproduced ECM. In the descrambling unit 5, the video packet and audio packet of the selected program are descrambled by using the scramble key. The separating unit 6 is controlled by the apparatus control unit 10 so as to select the data of the reproduced program. In a manner similar to the ordinary received program, the program by the reproduction data of the recording medium 20 can be monitored.

Although the example of transmitting the video and audio data through the broadcasting wave has been described above, similar techniques can be also applied to a system for transmitting the video and audio data by

a radio transmission other than the broadcasting wave. Only one of the video data and the audio data can be also transmitted. Further, data of a computer program can be also transmitted without limiting to the video and audio data.

By transmitting the data for retrieval to the viewer after the recording, the viewer can easily perform the selecting operation of the desired program.

Having described a specific preferred embodiment of the present invention with reference to the accompanying drawings, it is to be understood that the invention is not limited to that precise embodiment, and that various changes and modifications may be effected therein by one skilled in the art without departing from the scope of the invention as defined in the appended claims.

5

information data; and means for transmitting data to retrieve said plurality of information data and said present second control data after said plurality of encrypted data was transmitted.

4. A data receiving apparatus for receiving multiplexed digital data, wherein

10

a plurality of encrypted information data, first control data which is used to decrypt said encryption and is common to receiving terminals, and second control data which is used to decrypt said encryption and is individual for each of said receiving terminals are included in a reception signal,

and said apparatus comprises:

### Claims

1. A data transmitting apparatus for transmitting multiplexed digital data, comprising:

means for encrypting a plurality of information data; and  
means for transmitting first control data which is used to decrypt said encryption and is common to receiving terminals and second control data which is used to decrypt said encryption and is individual for each of said receiving terminals together with said plurality of encrypted information data.

20

recording means for recording said plurality of encrypted information data and said first control data;

a recording medium on which said plurality of encrypted information data and said first control data are recorded by said recording means;

reproducing means for reproducing said encrypted information data and said first control data which were recorded on said recording medium by said recording means; and

means for decrypting the encryption of said encrypted information data reproduced by said reproducing means by using said first control data reproduced by said reproducing means and said present second control data received.

2. A data transmitting apparatus for transmitting multiplexed digital data, comprising:

means for encrypting a plurality of information data;  
means for transmitting first control data which is used to decrypt said encryption and is common to receiving terminals and second control data which is used to decrypt said encryption and is individual for each of said receiving terminals together with said plurality of encrypted information data; and  
means for transmitting data to retrieve said plurality of information data.

35

5. A data receiving apparatus for receiving multiplexed digital data, wherein

3. A data transmitting apparatus for transmitting multiplexed digital data, comprising:

means for encrypting a plurality of information data;  
means for transmitting first control data which is used to decrypt said encryption and is common to receiving terminals and second control data which is used to decrypt said encryption and is individual for each of said receiving terminals together with said plurality of encrypted

40

recording means for recording said plurality of encrypted information data and said first control data;

a recording medium on which said plurality of encrypted information data and said first control data are recorded by said recording means;

managing means for instructing a recording position of each of said plurality of en-

50

55

50

55

- cryptic information data recorded on said recording medium by said recording means;  
reproducing means for reproducing desired encrypted information data and said first control data according to said information data with reference to said managing means from said plurality of encrypted information data and said first control data which were recorded on said recording medium by said recording means; and  
means for decrypting the encryption of said encrypted information data reproduced by said reproducing means by using said first control data reproduced by said reproducing means and said present second control data received.

5. A data receiving system for receiving multiplexed digital data, comprising:

a receiving apparatus having receiving means for receiving a plurality of encrypted information data, first control data which is used to decrypt said encryption and is common to receiving terminals, and second control data which is used to decrypt said encryption and is individual for each of said receiving terminals;  
a recording and reproducing apparatus;

20

transmitting means for transmitting said plurality of encrypted information data and said first control data which were received by said receiving means to said recording and reproducing apparatus; and  
transmitting means for transmitting said encrypted information data and said first control data which were recorded and reproduced by said recording and reproducing apparatus,

25

wherein said recording and reproducing apparatus has  
recording means for recording said plurality of encrypted information data and said first control data which were transmitted from said receiving apparatus by said transmitting means and  
reproducing means for reproducing said encrypted information data and said first control data which were recorded by said recording means, and  
said receiving apparatus has  
means for decrypting the encryption of said encrypted information data transmitted from said recording and reproducing apparatus by said transmitting means by using said first control data transmitted from said recording and reproducing apparatus by said transmitting means and said present second control data received.

30

35

40

45

50

55

60

65

70

75

80

85

90

95

100

105

110

115

120

125

130

135

140

145

150

155

160

165

170

175

180

185

190

195

200

205

210

215

220

225

230

235

240

245

250

255

260

265

270

275

280

285

290

295

300

305

310

315

320

325

330

335

340

345

350

355

360

365

370

375

380

385

390

395

400

405

410

415

420

425

430

435

440

445

450

455

460

465

470

475

480

485

490

495

500

505

510

515

520

525

530

535

540

545

550

555

560

565

570

575

580

585

590

595

600

605

610

615

620

625

630

635

640

645

650

655

660

665

670

675

680

685

690

695

700

705

710

715

720

725

730

735

740

745

750

755

760

765

770

775

780

785

790

795

800

805

810

815

820

825

830

835

840

845

850

855

860

865

870

875

880

885

890

895

900

905

910

915

920

925

930

935

940

945

950

955

960

965

970

975

980

985

990

995

1000

1005

1010

1015

1020

1025

1030

1035

1040

1045

1050

1055

1060

1065

1070

1075

1080

1085

1090

1095

1100

1105

1110

1115

1120

1125

1130

1135

1140

1145

1150

1155

1160

1165

1170

1175

1180

1185

1190

1195

1200

1205

1210

1215

1220

1225

1230

1235

1240

1245

1250

1255

1260

1265

1270

1275

1280

1285

1290

1295

1300

1305

1310

1315

1320

1325

1330

1335

1340

1345

1350

1355

1360

1365

1370

1375

1380

1385

1390

1395

1400

1405

1410

1415

1420

1425

1430

1435

1440

1445

1450

1455

1460

1465

1470

1475

1480

1485

1490

1495

1500

1505

1510

1515

1520

1525

1530

1535

1540

1545

1550

1555

1560

1565

1570

1575

1580

1585

1590

1595

1600

1605

1610

1615

1620

1625

1630

1635

1640

1645

1650

1655

1660

1665

1670

1675

1680

1685

1690

1695

1700

1705

1710

1715

1720

1725

1730

1735

1740

1745

1750

1755

1760

1765

1770

1775

1780

1785

1790

1795

1800

1805

1810

1815

1820

1825

1830

1835

1840

1845

1850

1855

1860

1865

1870

1875

1880

1885

1890

1895

1900

1905

1910

1915

1920

1925

1930

1935

1940

1945

1950

1955

1960

1965

1970

1975

1980

1985

1990

1995

2000

2005

2010

2015

2020

2025

2030

2035

2040

2045

2050

2055

2060

2065

2070

2075

2080

2085

2090

2095

2100

2105

2110

2115

2120

2125

2130

2135

2140

2145

2150

2155

2160

2165

2170

2175

2180

2185

2190

2195

2200

2205

2210

2215

2220

2225

2230

2235

2240

2245

2250

2255

2260

2265

2270

2275

2280

2285

2290

2295

2300

2305

2310

2315

2320

2325

2330

2335

2340

2345

2350

2355

2360

2365

2370

2375

2380

2385

2390

2395

2400

2405

2410

2415

2420

2425

2430

2435

2440

2445

2450

2455

2460

2465

2470

2475

2480

2485

2490

2495

2500

2505

2510

2515

2520

2525

2530

2535

2540

2545

2550

2555

2560

2565

2570

2575

2580

2585

2590

2595

2600

2605

2610

2615

2620

2625

2630

2635

2640

2645

2650

2655

2660

2665

2670

2675

2680

2685

2690

2695

2700

2705

2710

2715

2720

2725

2730

2735

2740

2745

2750

2755

2760

2765

2770

2775

2780

2785

2790

2795

2800

2805

2810

2815

2820

2825

2830

2835

2840

2845

2850

2855

2860

2865

2870

2875

2880

2885

2890

2895

2900

2905

2910

2915

2920

2925

2930

2935

2940

2945

2950

2955

2960

2965

2970

2975

2980

2985

2990

2995

3000

3005

3010

3015

3020

3025

3030

3035

3040

3045

3050

3055

3060

3065

3070

3075

3080

3085

3090

3095

3100

3105

3110

3115

3120

3125

3130

3135

3140

3145

3150

3155

3160

3165

3170

3175

3180

3185

3190

3195

3200

3205

3210

3215

3220

3225

3230

3235

3240

3245

3250

3255

3260

3265

3270

3275

3280

3285

3290

3295

3300

3305

3310

3315

3320

3325

3330

3335

3340

3345

3350

3355

3360

3365

3370

3375

3380

3385

3390

3395

3400

3405

3410

3415

3420

3425

3430

3435

3440

3445

3450

3455

3460

3465

3470

3475

3480

3485

3490

3495

3500

3505

3510

3515

3520

3525

3530

3535

3540

3545

3550

3555

3560

3565

3570

3575

3580

3585

3590

3595

3600

3605

3610

3615

3620

3625

3630

3635

3640

3645

3650

3655

3660

3665

3670

3675

3680

3685

3690

3695

3700

3705

3710

3715

3720

3725

3730

3735

3740

3745

3750

3755

3760

3765

3770

3775

3780

3785

3790

3795

3800

3805

3810

3815

3820

3825

3830

3835

3840

3845

3850

3855

3860

3865

3870

3875

3880

3885

3890

3895

3900

3905

3910

3915

3920

3925

3930

3935

3940

3945

3950

3955

3960

3965

3970

3975

3980

3985

3990

3995

4000

4005

4010

4015

4020

4025

4030

4035

4040

4045

4050

4055

4060

4065

4070

4075

4080

4085

4090

4095

4100

4105

4110

4115

4120

4125

4130

4135

4140

4145

4150

4155

4160

4165

4170

4175

4180

4185

4190

4195

4200

4205

4210

4215

4220

4225

4230

4235

4240

4245

4250

4255

4260

4265

4270

4275

4280

4285

4290

4295

4300

4305

4310

4315

4320

4325

4330

4335

4340

4345

4350

4355

4360

4365

4370

4375

4380

4385

4390

4395

4400

4405

4410

4415

4420

4425

4430

4435

4440

4445

4450

4455

4460

4465

4470

4475

4480

4485

4490

4495

4500

4505

4510

4515

4520

4525

4530

4535

4540

4545

4550

4555

4560

4565

4570

4575

4580

4585

4590

4595

4600

4605

4610

4615

4620

4625

4630

4635

4640

4645

4650

4655

4660

4665

4670

4675

4680

4685

4690

4695

4700

4705

4710

4715

4720

4725

4730

4735

4740

4745

4750

4755

4760

4765

4770

4775

4780

4785

4790

4795

4800

4805

4810

4815

4820

4825

4830

4835

4840

4845

4850

4855

4860

4865

4870

4875

4880

4885

4890

4895

4900

4905

4910

4915

4920

4925

4930

4935

4940

4945

4950

4955

4960

4965

4970

4975

4980

4985

4990

4995

5000

5005

5010

5015

5020

5025

5030

5035

5040

5045

5050

5055

5060

5065

5070

5075

5080

5085

5090

5095

5100

5105

5110

5115

5120

5125

5130

5135

5140

5145

5150

5155

5160

5165

5170

5175

5180

5185

5190

5195

5200

5205

5210

5215

5220

5225

5230

5235

5240

5245

5250

5255

5260

5265

5270

5275

5280

5285

5290

5295

5300

5305

5310

5315

5320

5325

5330

5335

5340

5345

5350

5355

5360

5365

5370

5375

5380

5385

5390

5395

5400

5405

5410

5415

5420

5425

5430

5435

5440

5445

5450

5455

5460

5465

5470

5475

5480

5485

5490

5495

5500

5505

5510

5515

5520

5525

5530

5535

5540

5545

5550

5555

5560

5565

5570

5575

5580

5585

5590

5595

5600

5605

5610

5615

5620

5625

5630

5635

5640

5645

5650

5655

5660

5665

5670

5675

5680

5685

5690

5695

5700

5705

5710

5715

5720

5725

5730

5735

5740

5745

5750

5755

5760

5765

5770

5775

5780

5785

5790

5795

5800

5805

5810

5815

5820

5825

5830

5835

5840

5845

5850

5855

5860

5865

5870

5875

5880

5885

5890

5895

5900

5905

5910

5915

5920

5925

5930

5935

5940

5945

5950

5955

5960

5965

5970

5975

5980

5985

5990

5995

6000

6005

6010

6015

6020

6025

6030

6035

6040

6045

6050

6055

6060

6065

6070

6075

6080

6085

6090

6095

6100

6105

6110

6115

6120

6125

6130

6135

6140

6145

6150

6155

6160

6165

6170

6175

6180

6185

6190

6195

6200

6205

6210

6215

6220

6225

6230

6235

6240

6245

6250

6255

6260

6265

6270

6275

6280

6285

6290

6295

6300

6305

6310

6315

6320

6325

6330

6335

6340

6345

6350

6355

6360

6365

6370

6375

6380

6385

6390

6395

6400

6405

6410

6415

6420

6425

6430

6435

6440

6445

6450

6455

6460

6465

6470

6475

6480

6485

6490

6495

6500

6505

6510

6515

6520

6525

6530

6535

6540

6545

6550

6555

6560

6565

6570

6575

6580

6585

6590

6595

6600

6605

6610

6615

6620

6625

6630

6635

6640

6645

6650

6655

6660

6665

6670

6675

6680

6685

6690

6695

6700

6705

6710

6715

6720

6725

6730

6735

6740

6745

6750

6755

6760

6765

6770

6775

6780

<p

9. A system according to claim 6, wherein after said plurality of encrypted information data and said first control data were recorded by said recording means, data for retrieving said plurality of information data is received together with said present second control data by said receiving apparatus, and desired information data is selectively reproduced by said reproducing means by using said data for retrieving. 5
10. A data transmission and reception system for transmitting multiplexed digital data and receiving said multiplexed digital data, wherein
- a transmission side has  
means for encrypting a plurality of information data and  
means for transmitting first control data which is used to decrypt said encryption and is common to receiving terminals and second control data which is used to decrypt said encryption and is individual for each of said receiving terminals together with said plurality of encrypted information data, and  
a reception side has  
recording means for recording said plurality of encrypted information data and said first control data,  
a recording medium on which said plurality of encrypted information data and said first control data are recorded by said recording means, reproducing means for reproducing said encrypted information data and said first control data which were recorded on said recording medium by said recording means, and  
means for decrypting the encryption of said encrypted information data reproduced by said reproducing means by using said first control data reproduced by said reproducing means and said present second control data received. 15 20 25 30 35 40
11. A data transmission and reception system for transmitting multiplexed digital data and receiving said multiplexed digital data, wherein
- a transmission side has  
means for encrypting a plurality of information data and  
means for transmitting first control data which is used to decrypt said encryption and is common to receiving terminals and second control data which is used to decrypt said encryption and is individual for each of said receiving terminals together with said plurality of encrypted information data, and  
a reception side has  
recording means for recording said plurality of encrypted information data and said first con- 45 50 55
- trol data,  
a recording medium on which said plurality of encrypted information data and said first control data are recorded by said recording means, managing means for instructing a recording position of each of said plurality of encrypted information data recorded on said recording medium by said recording means, reproducing means for reproducing desired encrypted information data and said first control data according to said information data with reference to said managing means from said plurality of encrypted information data and said first control data which were recorded on said recording medium by said recording means, and  
means for decrypting the encryption of said encrypted information data reproduced by said reproducing means by using said first control data reproduced by said reproducing means and said present second control data received.
12. A system according to claim 10, further comprising means for transmitting data for retrieving said plurality of information data together with said present second control data after said plurality of encrypted information data was transmitted.
13. A data transmission and reception system for transmitting multiplexed digital data and receiving said multiplexed digital data, wherein
- a transmission side comprises  
means for encrypting a plurality of information data and  
means for transmitting first control data which is used to decrypt said encryption and is common to receiving terminals and second control data which is used to decrypt said encryption and is individual for each of said receiving terminals together with said plurality of encrypted information data, and  
a reception side comprises  
a receiving apparatus having receiving means for receiving said plurality of encrypted information data, said first control data, and said second control data,  
a recording and reproducing apparatus,  
transmitting means for transmitting said plurality of encrypted information data and said first control data which were received by said receiving means to said recording and reproducing apparatus, and  
transmitting means for transmitting said encrypted information data and said first control data which were recorded and reproduced by said recording and reproducing apparatus to

- said receiving apparatus,  
said recording and reproducing apparatus  
comprises  
recording means for recording said plurality of  
encrypted information data and said first control  
data which were transmitted from said receiving  
apparatus by said transmitting means,  
and  
reproducing means for reproducing said en-  
crypted information data and said first control  
data which were recorded by said recording  
means, and  
said receiving apparatus has  
means for decrypting the encryption of said en-  
crypted information data transmitted from said  
recording and reproducing apparatus by said  
transmitting means by using said first control  
data transmitted from said recording and repro-  
ducing apparatus by said transmitting means  
and said present second control data.
14. A data transmission and reception system for trans-  
mitting multiplexed digital data and receiving said  
multiplexed digital data, wherein  
a transmission side comprises  
means for encrypting a plurality of information  
data and  
means for transmitting first control data which  
is used to decrypt said encryption and is com-  
mon to receiving terminals and second control  
data which is used to decrypt said encryption  
and is individual for each of said receiving ter-  
minals together with said plurality of encrypted  
information data, and  
a reception side comprises  
a receiving apparatus having receiving means  
for receiving said plurality of encrypted informa-  
tion data, said first control data, and said sec-  
ond control data,  
a recording and reproducing apparatus,  
transmitting means for transmitting said plural-  
ity of encrypted information data and said first  
control data which were received by said re-  
ceiving means to said recording and reproduc-  
ing apparatus, and  
transmitting means for transmitting said en-  
crypted information data and said first control  
data which were recorded and reproduced by  
said recording and reproducing apparatus to  
said receiving apparatus,  
said recording and reproducing apparatus  
comprises  
recording means for recording said plurality of  
encrypted information data and said first control  
data which were transmitted from said re-  
ceiving apparatus by said transmitting means,  
managing means for instructing a recording po-
- 5  
10  
15  
20  
25  
30  
35  
40  
45  
50  
55
- sition of each of said plurality of encrypted in-  
formation data recorded by said recording  
means, and  
reproducing means for reproducing desired en-  
crypted information data and said first control  
data according to said information data with ref-  
erence to said managing means from said plu-  
rality of encrypted information data and said  
first control data which were recorded by said  
recording means,  
said receiving apparatus has  
means for decrypting the encryption of said en-  
crypted information data transmitted from said  
recording and reproducing apparatus by said  
transmitting means by using said first control  
data transmitted from said recording and repro-  
ducing apparatus by said transmitting means  
and said present second control data.
15. A system according to claim 13, further comprising  
means for transmitting data for retrieving said  
plurality of information data together with said  
present second control data after said plurality  
of encrypted information data was transmitted.
16. An apparatus according to claim 1, wherein said  
digital data is a broadcasting wave of a digital tele-  
vision broadcasting.
17. An apparatus according to claim 4, wherein said  
digital data is a broadcasting wave of a digital tele-  
vision broadcasting.
18. A system according to claim 6, wherein said digital  
data is a broadcasting wave of a digital television  
broadcasting.
19. A system according to claim 10, wherein said digital  
data is a broadcasting wave of a digital television  
broadcasting.
20. A system according to claim 13, wherein said digital  
data is a broadcasting wave of a digital television  
broadcasting.
21. A system according to claim 6, wherein said record-  
ing and reproducing apparatus is a digital VCR.

Fig. 1

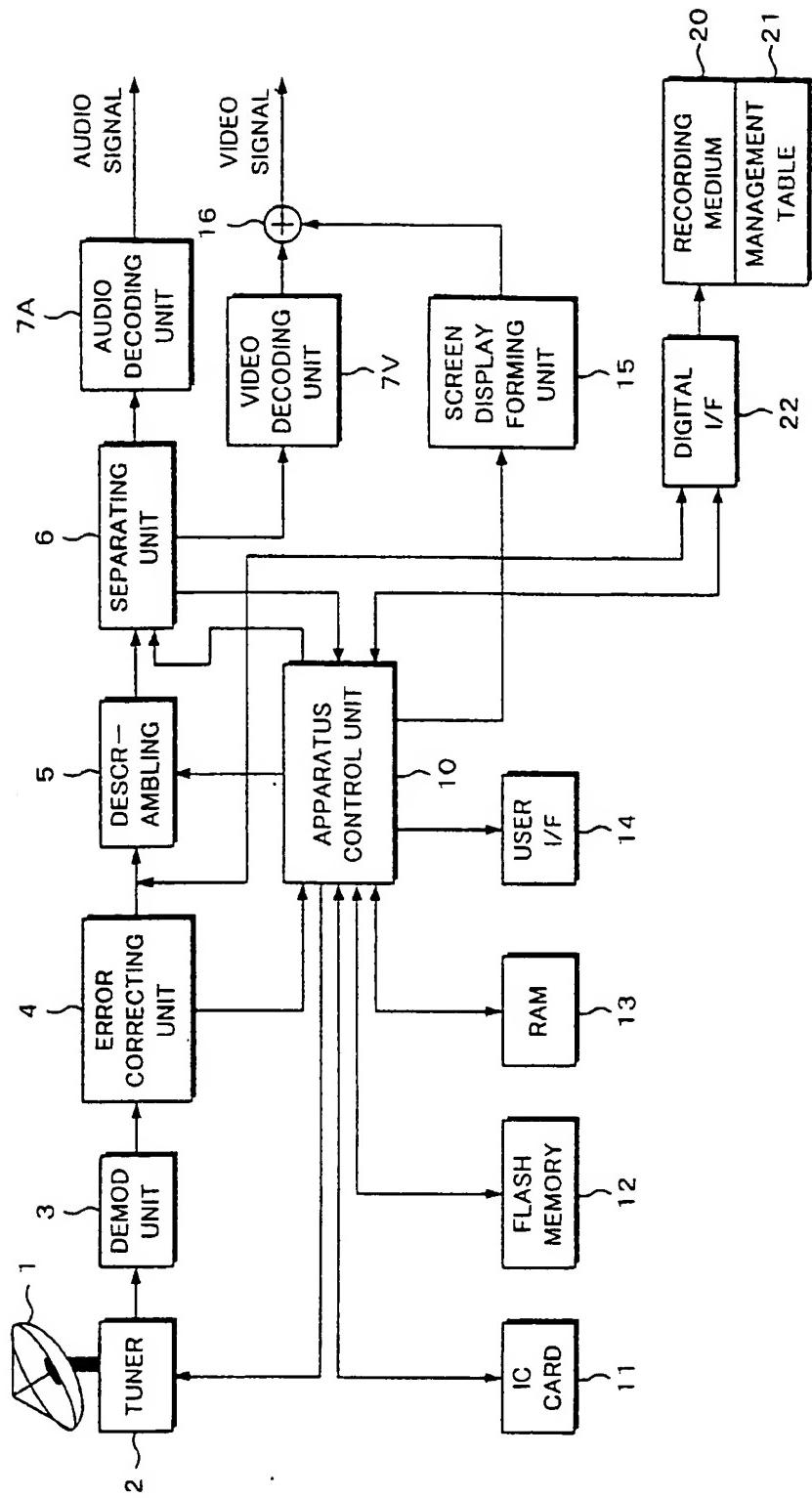
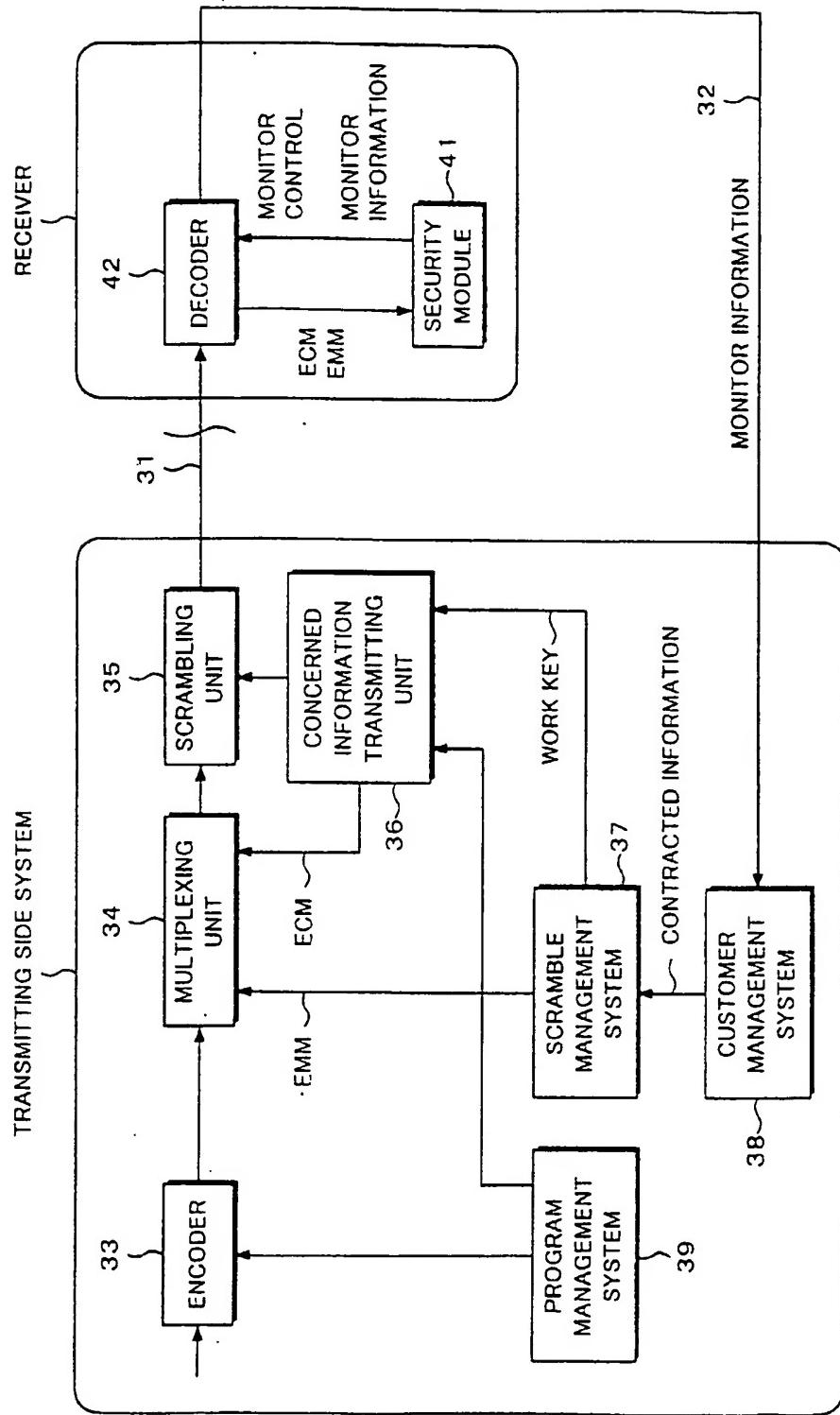


Fig. 2



*Fig. 3*

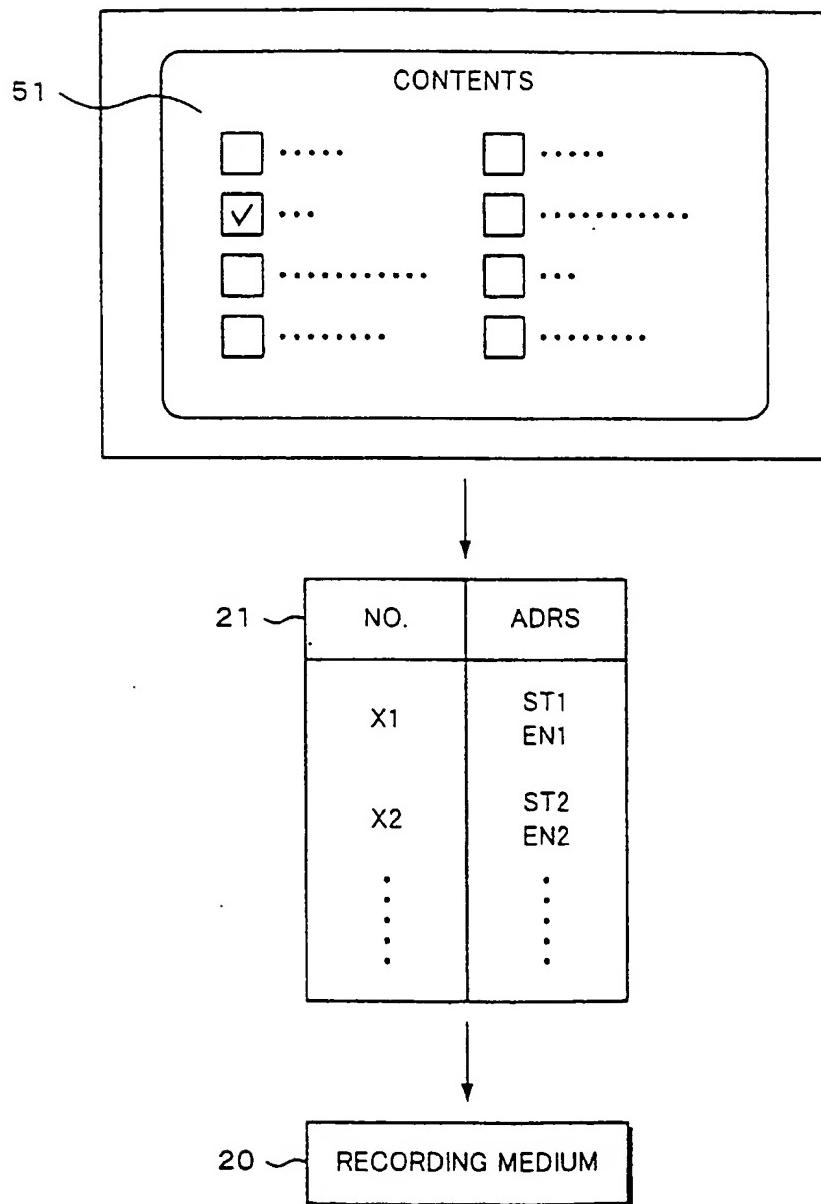


Fig. 4

